УДК 342:004.056.5
ББК 67.401:32.972.53

Шкодина Е.С., Шиханова Е.Г.
Самарский национальный исследовательский университет имени академика С.П. Королева, Самара

ПРАВОВОЕ РЕГУЛИРОВАНИЕ КИБЕРБЕЗОПАСНОСТИ: ПОСТАНОВКА ПРОБЛЕМЫ

Аннотация: Уровень киберпреступности по всему миру растет быстрыми темпами. Многие сферы жизнедеятельности находятся под угрозой. В статье рассматриваются такой феномен как кибербезопасность, также анализируются нормативно-правовые акты, регулирующие данный феномен. Авторами предложены некоторые пути решения данных проблем.

Ключевые слова: кибербезопасность, киберпреступления, кибер-угрозы, цифровизация, персональные данные.

Shkodina E. S., Shikhanova E. G.
Samara National Research University, Samara

CYBERSECURITY AS A LEGAL CATEGORY: PROBLEM STATEMENT

Abstract: The level of cybercrime around the world is growing rapidly. Many areas of life are under threat. The article deals with the main problems associated with cybercrime, as well as analyzes the legal acts regulating this phenomenon. The authors suggest some ways to solve these problems.

Keywords: cybersecurity, cybercrime, cyber threats, digitalization, personal data.

В современных условиях повсеместной цифровизации, крайне актуальной становится проблема кибербезопасности. Различные государственные, муниципальные и коммерческие структуры владеют огромными массивами информации. В условиях научно-технического прогресса изменяется количество и качество цифровых средств, которые способны считывать, анализировать, передавать и т.д. полученные данные с большой скоростью. Вслед за усилением интеграции между работой коммерческих учреждений и цифровых технологий появляются угрозы, которые открывают все больше новых путей для образования новых мошеннических схем. Обостряется проблема защиты персональных данных в связи с диджитализацией общества.

Слишком много информации попадает в интернет и хранится в различных облачных хранилищах вечно. Количество гаджетов, подключенных к интернету, с

каждым годом увеличивается в геометрической прогрессии. Многие программы берут разрешение у пользователей на использование данных и тем самым в процессе собирают не только основную информацию, необходимую для работы приложения, но и множество других персональных сведений.

Целью настоящей работы является выявление проблем, возникающих в процессе цифровой глобализации. В соответствие с чем, предполагается поэтапное решение следующих задач: конкретизация теоретических конструкций, используемых в работе; выявление основных проблем, возникающих в связи с цифровизацией различных отраслей; анализ нормативно-правовых актов, регулирующих правомерность использования информации; определение рисков и их минимизация.

Главы государств обеспокоены данной проблемой, так как киберугрозы могут нанести существенный вред национальной безопасности, в том числе безопасности граждан, экономике и другим институтам [5]. Именно поэтому крайне важно проводить эффективную политику кибербезопасности.

Проанализировав ряд мнений исследователей проблем кибербезопасности в современном обществе (Ищанова Р. К., Сафонова М.Ф., Ципляева С.А., Хлопов О.А. и др.), в настоящем исследовании авторы предлагают понимать под кибербезопасностью - совокупность методов, обеспечивающих защиту телекоммуникационных каналов, с помощью которых собирается, хранится и распространяется информация, от кибератак [1]. Так, докринально можно выделить ряд признаков: системность (совокупность методов); наличие информации, подлежащей защите; «материальная виртуальность» (защита телекоммуникационных каналов); наличие реальной или потенциальной угрозы (возможность кибератак); способность обеспечить защиту.

В настоящее время существует ряд нормативных актов, регулирующих отношения, связанные с информационной безопасностью. Одним из них является Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ. Данный акт включает в себя несколько положений, включающих информацию о безопасности данных в сети Интернет. Однако, как отмечают исследователи [6], влияние кибербезопасности распространяется не только на это направление. По нашему мнению, стоит уточнить некоторые формулировки, конкретизировать термин «кибербезопасность» и определить сферу его действия, так как данное понятие в настоящее время вышло за пределы существующего правового регулирования.

На данный момент, наиболее фундаментальным документом, определяющим различные направления кибербезопасности, является «Концепция стратегии кибербезопасности Российской Федерации». Однако, основной ее задачей является не регулирование правовых отношений, а «организация поддержки отечественных разработчиков программного обеспечения» [4].

Реальной или потенциальной угрозе информация подвергается посредством мошеннических действий. Правовое регулирование неправомерных действий, в данном случае, осуществляется в рамках УК РФ и КоАП РФ. Чаще всего для обмана мошенники используют социальные сети или средства коммуникации. На настоящий момент практически каждый человек сталкивался хотя бы с одним из видов кибермошенничества. Мошенники используют в диалогах личную информацию о потенциальной жертве, тем самым, «втираются» в доверие. Чаще всего, преступники еще до момента контакта уже знают необходимую информацию о человеке, остальную информацию получают в процессе разговора.

Был проведен эксперимент, в ходе которого людям были совершены звонки от человека, который представился работником банка, назвал имя клиента и последние цифры номера карты. Было выявлено, что 6 человек из 20 заинтересовались проблемой, озвученной в разговоре, а значит при дальнейшем бы общении продиктовали бы свои данные и, соответственно, стали бы жертвами киберпреступления [3].

Кроме мошенничества популярными киберпреступлениям является «продажа» и «утечка» информации. Таким образом, объективная сторона составов правонарушений отражает действие или бездействие. Во втором случае, оператор информации не обеспечил надлежащую защиту, т.е. кибербезопасность. Большинство утечек информации с персональными данными наблюдается в страховых организациях, в банках, у сотовых операторов, интернет-магазинов. В первом случае, недобросовестные работники таких организаций продают информационные базы мошенникам. И тот и другой вариант злоупотреблений требует новых вариативных методов решения проблемы.

Правительство предлагает повысить штрафы для организаций с 50 до 500 тысяч рублей. Однако, по нашему мнению, необходимо обновить требования к технической и правовой защите информации. Так как в данной ситуации компаниям проще заплатить штраф, нежели вносить изменения в систему управления и/или структуру компании.

Следует отметить, что обеспечение кибербезопасности осложняется недостатком компетентных специалистов на рынке труда. Именно, поэтому их востребованность настолько высока. Кроме того, еще острее стоит проблема расследования правонарушений. Профессиональное образование только встает на путь подготовки юристов в IT-сфере.

По нашему мнению, такое направление как кибербезопасность нуждается в целостной нормативной базе. Необходимо совершенствовать законодательство и своевременно актуализировать принятые нормы. Для этого должны работать компетентные специалисты, способные реализовывать законодательную функцию

на стыки двух профессий: юриста и IT-специалиста. В свою очередь, заинтересованным органам и организациям следует увеличить затраты на кибербезопасность. Для того, чтобы выстроить систему защиты информации в киберпространстве, в первую очередь, нужно оценить все риски и спрогнозировать возможные последствия [2], а для того, чтобы она была эффективной – своевременно ее актуализировать.

Библиографический список

1. Елизарова Е.О., Настич В.М., Чекулаев С.С. Правовое регулирование цифровой безопасности в России и странах АТР и ее соотношение с кибербезопасностью // Юридическая наука. 2020. №6. С. 42-46.

2. Ищанова Р. К. Обеспечение кибербезопасности // Большая Евразия: Развитие, безопасность, сотрудничество. 2019. №2-1. С. 367-368.

3. Сафонова М.Ф., Ципляева С.А. Кибербезопасность: проблемы и решения // ЕГИ. 2019. №24. С. 63-68..2020).

4. Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации»

5. Хлопов О.А. Проблемы кибербезопасности и защиты критической инфраструктуры // The Scientific Heritage. 2020. №45-5 (45). С. 64-69.

6. Цирлов В.Л. Правовые основы кибербезопасности Российской Федерации // Правовая информатика. 2013. №4. С. 66-68.